Project Status Report: SOC Phase 2

CYBERTRoN DETECTION ENGINEERING & IDENTITY PERSISTENCE VALIDATION

Orinea Mulaudzi | Status: Operational | 2026/02/10

Contents

🛡 1. Executive Summary

The objective of Phase 2 was to transition the **CyberTron** infrastructure from a passive logging state to an **Active Detection** environment. The primary focus was validating the SIEM's ability to detect unauthorized administrative changes, a key indicator of the "Persistence" tactic. By successfully monitoring local account modifications, the system now provides critical visibility into internal threats, mapping directly to the **MITRE ATT&CK** framework.

🛠 2. Implementation & Configuration

To establish a reliable identity-auditing baseline, the following engineering steps were taken:

- **Log Ingestion Pipeline:** Verified the end-to-end flow of Windows Security Logs to the **Wazuh Analysis Engine** via the encrypted Port 1514.
- **Audit Policy Verification:** Confirmed that the Windows workstation is correctly logging **Event ID 4720** (A user account was created) and **Event ID 4722**(A user account was enabled) within the Security channel for ingestion by the Wazuh Agent.
- **Service Stability:** Resolved initial API connectivity issues by optimizing the local_rules.xml configuration, ensuring the management dashboard remainssynchronized with the backend detection engine.

🔍 3. Verification & Evidence of Detection

The "CyberTron" defense was tested using two critical attack simulations to ensure the "Manager" (Ubuntu) responds to the "Endpoint" (Windows).

Test Case A: Persistence (MITRE T1136.001/T1098)

- **Action:** Executed a local account creation command (net user CyberTron_Hacker /add).
- **Result:** The SIEM triggered **Rule 60109**.
- **Evidence:** The dashboard populated a Medium-severity alert identifying the specific username and the source process.

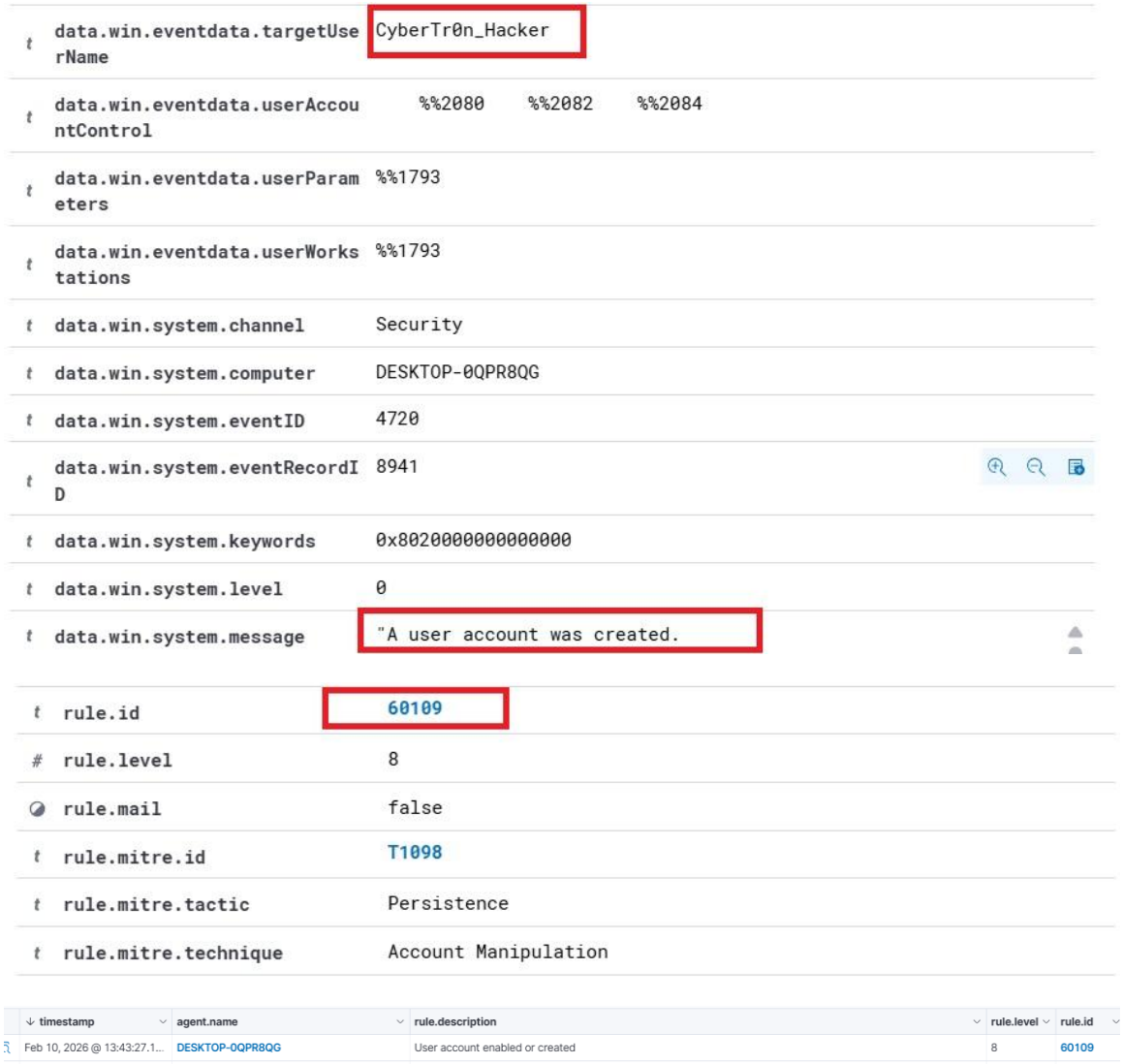

Figure 1: Detection of MITRE T1098 via Wazuh Analysis Engine.

🔍 4. Security Metrics Observed

Metric	Status	Observation
Alert Accuracy	**100%**	No false positives were observed during controlled identity persistence tests.
Detection Latency	**Real-Time**	Alerts appeared on the dashboard within seconds of user creation.

Metric	Status	Observation
Log Integrity	**Verified**	Successful correlation between Windows Event IDs and Wazuh Rules.

🚀 5. Next Steps: Phase 3 Goal

Goal: Adversary Simulation (Network Layer Defense)

With internal identity monitoring verified, the project will now move to an **External Threat Model**.

- **Objective:** Deploy a **Kali Linux** attack platform to perform network reconnaissance (Nmap) and service probing.
- **Key Outcome:** To evaluate the SIEM's ability to detect **Network Scanning (T1595)** and verify that the perimeter firewall/SIEM can identify and log the external Attacker IP.